3 cybersecurity priorities for your energy portfolio in 2026

Dear partners,

As we enter 2026, the digital layer of our energy system has become just as critical as the copper in the ground. The digitalization of energy infrastructure introduces powerful capabilities for trading and flexibility, but it also creates new vulnerabilities. At Withthegrid, we believe a resilient energy ecosystem must be built on a foundation of security and trust.

Based on recent developments in the field, we want to share three top priorities to secure your operations in the coming year.

Check your on-site firewalls: active scanning warning

We are seeing an increase in active scanning targeting the energy sector. Specifically, automated scripts are searching for routers with port forwarding enabled, which can expose internal services to attacks. If an attacker can reach your asset, they can control it.

☑ **The measure: Audit your installation sites immediately. Ensure that only required services are exposed through port forwarding, and closely monitor traffic on these ports using a strictly configured firewall.**

How the Teleport helps: The Teleport does not accept connections, thus significantly reducing the attack surface.

Update router and switch firmware

Hardware installed on remote sites is often treated as "set and forget." However, missing software updates creates a barrier full of holes: your system becomes full of newly found security vulnerabilities waiting to be exploited. Outdated network equipment is a common entry point for attackers looking to pivot into your wider control network.

☑ **The measure: Establish a routine maintenance schedule to update the firmware on all on-site routers and switches.**

How the Teleport helps: We manage all firmware for the Teleport directly. We securely deploy security patches remotely using automated, authenticated systems, ensuring the device is protected against new vulnerabilities without you needing to send a technician to the site.

Lock the front door: strong password, enable MFA everywhere

Human error remains a common entry point. A weak or compromised password should not be enough to take down a power plant.

☑ **The measure: Enforce Multi-Factor Authentication (MFA) across your organization. Treat it as a non-negotiable layer of defense that buys you time if credentials are ever leaked.**

How the Teleport helps: The Teleport Cloud Console supports role-based access control (RBAC) and strong authentication principles, allowing you to grant specific permissions to your team members without compromising security.

Next step

Security is a shared responsibility. If you are currently conducting a risk assessment for NIS2/Cbw (Cyberbeveiligingswet) compliance and need documentation regarding the Teleport's security controls, please contact info@withthegrid.com.
We are ready to support you.